APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/082,600	02/22/2002	David W. Grawrock	42390.P13484	5737

7590   11/21/2007

Jeffrey B. Huter
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER
SHERKAT, AREZOO

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
11/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/01/2007*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 9-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment received on

11/01/2007. Claims 1-44 are pending.

Response to Arguments

Applicant's arguments with respect to inaccurate citing of Hardy's disclosure has

been considered and is persuasive. Please find the corrected citings as follows:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6 and 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Hardy et al., (U.S. Publication No. 2002/0152392 and Hardy hereinafter), in view of

Davies, (U.S. Patent No. 4,799,258).

Regarding claims 1 and 9, Hardy discloses a method comprising:

requesting a first token (i.e., token storage medium 16) [to unseal a sealed first portion

of a multi-token sealed object] to obtain a first portion of the multi-token sealed object

(i.e., to calculate/generate split A), requesting a second token (i.e., the internal non-

volatile memory 12) [to unseal a sealed second portion of a multi-token sealed object] to obtain a second portion of the multi-token sealed object (i.e., split A), and using the first portion and the second portion to obtain an object from the multi-token sealed object (i.e., using split A and token to calculate/generate key A)(par. 14-24).

Hardy does not disclose sealing and unsealing of the first and the second portion.

However, Davies discloses an enciphered message relating to capabilities [of a computer system], stored in a tamper-resistant store of circuit contained by a token. The store also holds a secret key (i.e., private key) of a public key encryption system so that the enciphered message and the distinctive message can be transformed (i.e., signed/sealed) using the secret key and passed to the computer (i.e., in page 11 of the specification, it is disclosed that the process of sealing and unsealing is in fact encrypting the object to be sealed using an asymmetric cryptographic algorithm and the public token key sk)(col. 1, lines 65-67 and col. 2, lines 1-6 and col. 5, lines 60-67 and col. 6, lines 1-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Hardy with teachings of Davies because it would allow including sealing/transforming and unsealing/inverse transforming of the first and the second portion as disclosed by Davies. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Davies to prevent illegal manipulation of

"capabilities", so that "capabilities" are not allowed outside the computer's protected

store (Davies, col. 1, lines 5-22).

Regarding claim 10, Hardy discloses a method comprising

requesting a plurality of tokens to unseal a plurality sealed portions of a multi-

token sealed object, receiving a plurality of unsealed portions of the multi-token sealed

object (i.e., the required first portion, split A, and second portion token are

provided/generated by the first and second token), and obtaining an object that has

been sealed to the plurality of tokens using the plurality of unsealed portions of the

multi-token sealed object (i.e., the first portion and the second portion together generate

key A that decrypts the software corresponding to the claimed object)(par. 14-24).

Hardy does not disclose sealing and unsealing of the first and the second

portion.

However, Davies discloses an enciphered message relating to capabilities [of a

computer system], stored in a tamper-resistant store of circuit contained by a token.

The store also holds a secret key (i.e., private key) of a public key encryption system

so that the enciphered message and the distinctive message can be transformed

(i.e., signed/sealed) using the secret key and passed to the computer (i.e., in page

11 of the specification, it is disclosed that the process of sealing and unsealing is in

fact encrypting the object to be sealed using an asymmetric cryptographic algorithm

and the public token key sk)(col. 1, lines 65-67 and col. 2, lines 1-6 and col. 5, lines 60-67 and col. 6, lines 1-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Hardy with teachings of Davies because it would allow including sealing/transforming and unsealing/inverse transforming of the first and the second portion as disclosed by Davies. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Davies to prevent illegal manipulation of "capabilities", so that "capabilities" are not allowed outside the computer's protected store (Davies, col. 1, lines 5-22).

Regarding claim 2, the combined teachings of Hardy and Davies discloses the method of claim 1 further comprising obtaining the object of the multi-token sealed object by using the first portion as a key to decrypt the second portion (i.e., calculate other of split A or token using key A such that split A = key A $\oplus$ token)(fig. 2 – par. 14-24).

Hardy does not disclose sealing and unsealing of the first and the second portion.

However, Davies discloses an enciphered message relating to capabilities [of a computer system], stored in a tamper-resistant store of circuit contained by a token. The store also holds a secret key (i.e., private key) of a public key encryption system so that

the enciphered message and the distinctive message can be transformed (i.e., signed/sealed) using the secret key and passed to the computer (i.e., in page 11 of the specification, it is disclosed that the process of sealing and unsealing is in fact encrypting the object to be sealed using an asymmetric cryptographic algorithm and the public token key sk)(col. 1, lines 65-67 and col. 2, lines 1-6 and col. 5, lines 60-67 and col. 6, lines 1-67).

Regarding claim 3, the combined teachings of Hardy and Davies discloses the method of claim 1 further comprising receiving a key in response to the first token unsealing the sealed first portion, receiving an encrypted object in response to the second token unsealing the second portion, and obtaining the object of the multi-token sealed object by using the key to decrypt the encrypted object.

Hardy does not disclose sealing and unsealing of the first and the second portion.

However, Davies discloses an enciphered message relating to capabilities [of a computer system], stored in a tamper-resistant store of circuit contained by a token. The store also holds a secret key (i.e., private key) of a public key encryption system so that the enciphered message and the distinctive message can be transformed (i.e., signed/sealed) using the secret key and passed to the computer (i.e., in page 11 of the specification, it is disclosed that the process of sealing and unsealing is in fact encrypting the object to be sealed using an asymmetric cryptographic algorithm and the

public token key sk)(col. 1, lines 65-67 and col. 2, lines 1-6 and col. 5, lines 60-67 and

col. 6, lines 1-67).

Regarding claim 4, the combined teachings of Hardy and Davies discloses the

method of claim 1 further comprising generating a key based upon the first portion and

the second portion of the multi-token sealed object, and obtaining the object of the

multi-token sealed object by using the generated key to decrypt an encrypted object of

the multi-token sealed object.

Hardy does not disclose sealing and unsealing of the first and the second

portion.

However, Davies discloses an enciphered message relating to capabilities [of a

computer system], stored in a tamper-resistant store of circuit contained by a token. The

store also holds a secret key (i.e., private key) of a public key encryption system so that

the enciphered message and the distinctive message can be transformed (i.e.,

signed/sealed) using the secret key and passed to the computer (i.e., in page 11 of the

specification, it is disclosed that the process of sealing and unsealing is in fact

encrypting the object to be sealed using an asymmetric cryptographic algorithm and the

public token key sk)(col. 1, lines 65-67 and col. 2, lines 1-6 and col. 5, lines 60-67 and

col. 6, lines 1-67).

Regarding claim 5, the combined teachings of Hardy and Davies discloses the method of claim 1 further comprising generating a key from the first portion and the second portion of the multi-token sealed object, and obtaining the object of the multi-token sealed object by using the generated key and an a symmetric cryptographic algorithm to decrypt an encrypted object of the multi-token sealed object.

Hardy does not disclose sealing and unsealing of the first and the second portion.

However, Davies discloses an enciphered message relating to capabilities [of a computer system], stored in a tamper-resistant store of circuit contained by a token. The store also holds a secret key (i.e., private key) of a public key encryption system so that the enciphered message and the distinctive message can be transformed (i.e., signed/sealed) using the secret key and passed to the computer (i.e., in page 11 of the specification, it is disclosed that the process of sealing and unsealing is in fact encrypting the object to be sealed using an asymmetric cryptographic algorithm and the public token key sk)(col. 1, lines 65-67 and col. 2, lines 1-6 and col. 5, lines 60-67 and col. 6, lines 1-67).

Regarding claim 6, the combined teachings of Hardy and Davies discloses the method of claim 1 further comprising receiving a first key in response to the first token unsealing the sealed first portion, receiving a second key in response to the second token unsealing the second portion, generating a third key from the first key and the

second key, and obtaining the object of the multi-token sealed by using the third key to

decrypt an encrypted object of the multi-token sealed object.

Hardy does not disclose sealing and unsealing of the first and the second

portion.

However, Davies discloses an enciphered message relating to capabilities [of a

computer system], stored in a tamper-resistant store of circuit contained by a token. The

store also holds a secret key (i.e., private key) of a public key encryption system so that

the enciphered message and the distinctive message can be transformed (i.e.,

signed/sealed) using the secret key and passed to the computer (i.e., in page 11 of the

specification, it is disclosed that the process of sealing and unsealing is in fact

encrypting the object to be sealed using an asymmetric cryptographic algorithm and the

public token key sk)(col. 1, lines 65-67 and col. 2, lines 1-6 and col. 5, lines 60-67 and

col. 6, lines 1-67).

Regarding claim 11, the combined teachings of Hardy and Davies discloses the

method of claim 10 wherein obtaining comprises generating a key from the plurality of

unsealed portions of the multi-token sealed object, and decrypting an encrypted object

using the key to obtain the object.

Hardy does not disclose sealing and unsealing of the first and the second

portion.

However, Davies discloses an enciphered message relating to capabilities [of a computer system], stored in a tamper-resistant store of circuit contained by a token. The store also holds a secret key (i.e., private key) of a public key encryption system so that the enciphered message and the distinctive message can be transformed (i.e., signed/sealed) using the secret key and passed to the computer (i.e., in page 11 of the specification, it is disclosed that the process of sealing and unsealing is in fact encrypting the object to be sealed using an asymmetric cryptographic algorithm and the public token key sk)(col. 1, lines 65-67 and col. 2, lines 1-6 and col. 5, lines 60-67 and col. 6, lines 1-67).

Regarding claim 12, the combined teachings of Hardy and Davies discloses the method of claim 10 wherein obtaining comprises generating a key from the plurality of unsealed portions of the multi-token sealed object, and decrypting an encrypted object using the key and a symmetric cryptographic algorithm to obtain the object.

Hardy does not disclose sealing and unsealing of the first and the second portion.

However, Davies discloses an enciphered message relating to capabilities [of a computer system], stored in a tamper-resistant store of circuit contained by a token. The store also holds a secret key (i.e., private key) of a public key encryption system so that the enciphered message and the distinctive message can be transformed (i.e., signed/sealed) using the secret key and passed to the computer (i.e., in page 11 of the

specification, it is disclosed that the process of sealing and unsealing is in fact

encrypting the object to be sealed using an asymmetric cryptographic algorithm and the

public token key sk)(col. 1, lines 65-67 and col. 2, lines 1-6 and col. 5, lines 60-67 and

col. 6, lines 1-67).

Conclusion

The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure. Please see the attached PTO-892 for a complete listing.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-

3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.
Patent Examiner
Group 2131
Nov. 16, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100